Abstracts

Keynote talks

John Butcher

(University of Auckland, butcher@math.auckland.ac.nz)

Taylor series – pure and simple: The order of numerical methods for ordinary differential equations

A Runge–Kutta method takes small time steps, to approximate the solution to an initial value problem. How accurate is this approximation? If the error is asymptotically proportional to h^p, where h is the stepsize, the Runge–Kutta method is said to have "order" p. To find p, write the exact solution, after a single time-step, as a Taylor series, and compare with the Taylor series for the approximation.

This seems to be the answer to finding numerical orders – it is the truth pure and simple. But, this answer is too glib; "The truth is rarely pure and never simple".

Perhaps surprisingly, the order of a numerical method, for a scalar problem $y' = f(x,y)$, can be greater than when the same method is applied to a high-dimensional problem $y' = f(y)$. A consideration of the group structure of Runge–Kutta methods, leads to a more general definition of order. Methods that possess this enhanced "effective order", lead to genuinely improved numerical performance. Furthermore, the Hopf Algebra of rooted trees, which is at the heart of Runge–Kutta theory, turns out to be the appropriate basis for the order analysis of multi-stage multi-value numerical methods.

Michael Eastwood

(Australian National University, meastwoo@member.ams.org)

Invariant differential operators on the sphere

The circle is acted upon by the rotation group SO(2) and there are plenty of differential operators invariant under this action. But the circle is also acted upon by SL(2,R) and this larger symmetry group cuts down the list of invariant differential operators to something smaller but more interesting! I shall explain what happens and how this phenomenon generalises to spheres. These constructions are part of a general theory but have numerous unexpected applications, for example in suggesting a new stable finite-element scheme in linearised elasticity (due to Arnold, Falk, and Winther).

Andre Nies

(University of Auckland, andre@cs.auckland.ac.nz)

Interactions of computability and randomness

Randomness and complexity are closely connected. We provide mathematical counterparts of the two concepts for infinite sequences of bits. Then we discuss mathematical theorems showing the close relationship between the two concepts.

For a mathematician, randomness of an infinite sequence of bits (equivalently, a real) is usually understood probability-theoretically. Theorems about random objects hold outside some unspecified null class; for instance, a function of bounded variation is differentiable at every ”random” real. One cannot say that an individual real is random.

In algorithmic randomness one introduces a notion of effective null class. A sequence is random in that sense if it avoids each effective null class. For instance, Chaitin’s halting probability is random in the sense of Martin-Loef. A real is Martin-Loef random if and only if every computable function of bounded variation is differentiable at the real (Demuth 1975; recent work of Brattka, Miller and Nies).

Effective randomness notions interact in fascinating ways with the computational complexity of sequences of bits. For instance, being far from Martin-Loef random is equivalent to being close to computable in a specific sense (Nies, Advances in Math, 2005).

Jacqui Ramagge

(University of Wollongong, ramagge@uow.edu.au)

Using linear algebra when you only have groups

In 1994 George Willis introduced highly innovative tools which have revolutionized the study of locally compact groups. He essentially provided analogues of linear-algebraic concepts such as eigenvalues and eigenspaces in a context that is group-theoretic rather than linear in nature.

Each locally compact group is an extension of a connected group by a totally disconnected group. Connected, locally compact groups can be approximated by Lie groups and we therefore know a lot about them. In contrast, little was known about general totally disconnected, locally compact groups until recently. The study of Lie groups relies heavily on the use of Lie algebras and linear-algebraic concept. Willis’ theory enables us to transfer some results for connected locally compact groups into the totally disconnected case.

I will give an introduction to Willis’ key ideas, give an overview of what has been achieved so far, and identify directions for future research.

Hamish Spencer
(University of Otago, h.spencer@otago.ac.nz)

Using mathematical models to predict the evolution of genomic imprinting

In mammals, both paternally and maternally inherited copies of most genes are expressed. For a small number of genes, however, just the paternal copy is active, whereas in other cases only the maternal gene is transcribed. This form of non-Mendelian expression, known as genomic imprinting, amounts to functional haploidy, which appears paradoxical: why bother having two copies of a gene if you only use one? Different researchers have proposed a number of evolutionary explanations for how this form of gene expression might have evolved. The best-known suggestion, David Haig's "genetic conflict hypothesis", argues that imprinting arose as a response to the different genetic interests of mothers and fathers in organisms with multiple paternity and extensive post-fertilization maternal investment. A second suggestion, the "ovarian time-bomb hypothesis", holds that imprinting arose to prevent ovarian cancer. The verbal predictions of these hypotheses are often vague and overlapping. I will use mathematical models to tighten some of these predictions and to derive novel, unforeseen consequences of these ideas. My models thus allow us to decide which of these hypotheses are more likely to apply in nature.

Contributed talks

Astrid an Huef

(University of Otago, astrid@maths.otago.ac.nz)

Diagonals in C^*-algebras

A diagonal in a C^*-algebra A is a maximal abelian subalgebra B of A with properties modeled on those of $M_n(\mathbb{C})$ and its subalgebra of diagonal matrices. A Fell algebra is a C^*-algebra generated by its abelian elements. It turns out that every Fell algebra is almost a C^*-algebra with a diagonal. Also, diagonals in Fell algebras A can be characterised as the abelian subalgebras B which have the extension property relative to A (every pure state of B extends uniquely to a pure state of A). This is joint work with Alex Kumjian and Aidan Sims.

Gonzalo Aranda Pino

(University of Malaga, Spain, g.aranda@uma.es)

Weakly regular and self-injective Leavitt path algebras

Leavitt path algebras arise on the one hand from the algebras constructed by W. G. Leavitt to produce rings which do not satisfy the IBN property, and on the other hand from graph C^*-algebras, their analytic counterpart and descendant from the algebras investigated by J. Cuntz. In this talk we characterize the Leavitt path algebras over arbitrary graphs which are weakly regular rings as well as those which are self-injective. Concretely, for an arbitrary graph E and a field K we show the following:

- The Leavitt path algebra $L_K(E)$ is left (right) weakly regular if and only if the graph E satisfies Condition (K), and

- $L_K(E)$ is left (right) self-injective if and only if the graph E is row-finite, acyclic and every infinite path contains a line point.

This is a joint work with K. L. Rangaswamy and M. Siles Molina.

Michael Atkinson

(University of Otago, mike@cs.otago.ac.nz)

Bubblesort, stacks and permutations

Two simple sorting processes will be presented: single pass bubblesort and stacksort. The permutations that they sort can be described using pattern classes of permutations (which are sets of permutations defined by forbidding certain configurations in the permutations). After reprising the basic theory of pattern classes the bubblesort operator B will be analysed in terms of its effect on arbitrary pattern classes. In particular those pattern classes P for which $B^{-1}P$ is also a pattern class will be characterised. Finally the result will be applied to give a result on combining single sort bubblesort and stacksort.

This work is joint with Michael Albert, Mathilde Bouvel, Anders Claesson and Mark Dukes.

Boris Baeumer

(University of Otago, bbaeumer@maths.otago.ac.nz)

Parallel splitting and tempered operator stable random variables

Generating operator stable random variables with a non-trivial spectral measure is not straightforward. Usually sample paths of an operator stable motion are approximated using random vectors that are in the domain of attraction of the operator stable. Exponentially tempered random vectors have been introduced in large part to head off criticism of models that use stable processes as they usually have non-physical infinite moments. However having finite moments forces the tempered random vectors into the domain of attraction of the Gaussian, making a more detailed analysis of the above approximation method necessary in order to show that the approximate sample paths still mimic the behaviour of the tempered operator stable motion and that particle tracking codes do what they were designed to do. In the process we discover a convergence result for solving parabolic PDE's using parallel operator splitting.

Bill Barton

(University of Auckland, l.sheryn@math.auckland.ac.nz)

Implementing the pleasure principle

How can we give undergraduate students experiences that introduce them to the pleasures (and tribulations) of mathematical investigation and research? In current economies of scale, we can only do this by reducing lectures and shifting the focus away from examination-type questions and skills. I will argue that not only would this be useful in producing better undergraduates, but also that it would be more efficient pedagogically. I will outline a specific plan for a different philosophy and orientation to the undergraduate experience that is to be implemented at The University of Auckland–one that has them doing mathematics, not exercises, and handing responsibility to the students for a lot of routine learning.

Alona Ben-Tal

(Massey University, a.ben-tal@massey.ac.nz)

The power of many: Coupled pacemaker neurons in the pre-Bötzinger complex

The pre-Bötzinger complex is an area of the brainstem that generates rhythmic excitatory drive in the respiratory network during inspiration. Although studied extensively in the past decade there are still many features of the real system that are unknown. We have studied the dynamics of 1-, 2-, 3- and many-cells network theoretically and numerically and explored how the structure of the network and the number of cells affect the dynamics.

Luke Bennetts

(University of Otago, lbennetts@maths.otago.ac.nz)

Wave attenuation through multiple rows of scatterers with differing periodicities

Multiple-row arrays provide a computationally manageable means of calculating a wave field traveling through a vast number of scatterers. They have been used for problems in acoustics, electromagnetics and fluid dynamics. Most recently, they have been applied to make inferences about wave attenuation in the marginal ice zone. To facilitate the solution procedure, it is usually assumed that the periodicities in each row are identical. However, this produces some unwanted features in the attenuation that they predict. In this talk a solution method will be proposed for a multiple-row array in which the periodicities of the rows are allowed to differ. Results will be shown to demonstrate the smoothing effect this has on the transmitted wave field.

Anuj Bhowmik

(Auckland University of Technology, anuj.bhowmik@aut.ac.nz)

Existence of a Radner Equilibrium in infinite dimensional spaces

In 1968, Radner introduced exchange economies with differential (or asymmetric) information. In his model, an economy consists of a finite set of agents, each of whom is characterized by a state dependent utility function, a random initial endowment, a private information set and a prior belief. In this framework, agents make contingent contracts for trading commodities before they obtain any information about the realized state of nature. Such an economy is a generalization of the classical deterministic economy formulated rigorously by Arrow, Debreu and McKenzie in the 1950s.

In this talk, we consider the infinite dimensional space ℓ^∞ of bounded real sequences as the commodity space and extend a finite dimensional Radner competitive equilibrium to this infinite dimensional setting. In particular, the mathematical approach for the existence of a Radner competitive equilibrium in this setting will be highlighted. This is a recent joint work with J. Cao.

Kevin Broughan

(University of Waikato, kab@waikato.ac.nz)

Some recent advances on the perfect number problem

A perfect number is equal to the sum of its proper divisors. A multiperfect number is one which divides its sum of divisors. That there are no odd perfect (or multiperfect) numbers is the oldest open problem in mathematics.

In 2000 Florian Luca showed that no Fibonacci or classical Lucas number is perfect. In 2001 he showed that the same is true in general Lucas sequences with odd parameters. In 2009 he and 5 other authors, including Broughan, showed in a tour-de-force descent, that no Fibonacci number is multiperfect. Paul Pollack showed in 2010 that no odd repdigit, i.e. a number with all digits identical, to base 10 is perfect and this was extended by Luca and Pollack to odd multiperfect numbers in the same year. Zhou and

Broughan extended Pollack's result to all bases, 2 through 9, also in 2010.

I will give some details on how one or two of these results have been obtained and indicate why they might lead to a (partial!) resolution of the odd perfect number problem.

Jiling Cao

(Auckland University of Technology, jiling.cao@aut.ac.nz)

Wijsman Convergence: Topological properties and embedding

In 1966, when R. A. Wijsman studied some optimum properties of the sequential probability ratio test, he considered a mode of convergence for sequences of closed convex sets in $\mathbb{R}^n$. Since then, this type of convergence has attracted the attention of both analysts and topologists, and its applications in convex analysis and Banach space geometry have been explored.

Despite of investigation on Wijsman convergence in the past 40 years, some fundamental questions concerning its topology remain unsolved. For example, when does the Wijsman topology have the Baire property? When is the Wijsman topology normal? To attack these questions, the techniques of splitting and embedding have been employed. In this talk, I shall highlight recent progress towards these questions. In particular, some partial solutions and my recent joint work with H. J. K. Junnila, A. H. Tomita et al will be presented.

Tuan-Yow Chien

(University of Auckland, tchi043@aucklanduni.ac.nz)

Classifying harmonic frames up to unitary equivalence

Frame theory provides a way to generalise some familiar concepts in linear algebra in ways that have seen uses in signal processing and quantum information theory amongst other things. In particular a tight frame is in a way a natural generalisation of orthonormal bases. These objects can be constructed through relationships with groups, and we explore one way to classify harmonic frames up to unitary equivalence.

Hyuck Chung

(Auckland University of Technology, hchung@aut.ac.nz)

Flexural wave propagation in a semi-infinite floating plate under an edge loading

Numerical computation of flexural motion of a floating elastic plate is often complicated. The linear approximation of the motion makes the computation tractable for simple harmonic waves in a plate. I will introduce a few examples of the linear solution methods from various researchers. This talk will show how the Wiener-Hopf technique gives solutions for a semi-infinite plate with a sinusoidal edge loading. The solution is nearly explicit, which lets us analyze the dynamics of the plate for many frequencies in time and space along the edge. Certain distributions of edge loading can approximate a localized forcing on the edge. Then, the Wiener-Hopf technique can be used to find the response to a localised force at the edge of the plate. The resulting solutions may be used to find the relationship between the deflection and velocity near the location of forcing.

Megan Clark, Louise Sheryn

(Victoria University, megan.clark@msor.vuw.ac.nz)

Collective dreaming: A school-university interface

In 2008 the New Zealand Institute of Mathematics and Its Applications (NZIMA) funded a project to take a hard look at mathematics education in the four years from the last two years of secondary education to the first two years of undergraduate university education. The structure, pedagogy and content of mathematics in this period have been largely driven by tradition and particular interest groups. However not only has mathematics changed, but also the student body has changed, the teaching and lecturing body has changed, the reasons people study the mathematical sciences has changed, and the mathematical preliminaries have changed. The prime aim of the project was to get mathematical science senior secondary teachers and undergraduate lecturers to talk to each other. Such communication has not happened before in New Zealand on a large scale, and the conventional mythologies are couched in terms of blame and complaint. We explain why we think the project overcame these obstacles and describe the emerging vision.

Marston Conder

(University of Auckland, m.conder@auckland.ac.nz)

Large groups acting on surfaces of given genus, and the symmetric genus of a given group

This talk will concentrate on recent developments with regard to these questions: What is the *largest number of automorphisms* of

- a compact orientable surface of given genus $g > 1$?
- a compact non-orientable surface of given genus $g > 2$?

Given a finite group G, what is the *smallest genus of faithful actions* of G on

- compact orientable surfaces?
- compact orientable surfaces, preserving orientation?
- compact non-orientable surfaces?

Some of what I will report is joint work with Tom Tucker (New York).

John Curran
(University of Otago, jcurran@maths.otago.ac.nz)

A smallest complete group of odd order

A group is said to be complete if its centre is trivial and it is isomorphic to its automorphism group.

Complete groups are regarded by group theorists as somewhat of an oddity and are relatively rare. However they have a long history, and as far back as 1895, Hölder showed that the symmetric group S_n is complete, except when $n = 2$ or $n = 6$. Other examples followed but they were also of even order. Dark (1975) produced the first complete group of odd order $(3.19.7^{12})$. Others have since been found, with the smallest of order $3^{12}.5$ (Heineken, 1996).

In this talk, I will say a little about complete groups and mention a recent result (Curran, Dark): That a relative holomorph of a certain p-group P of order p^5, $p \equiv 1 \pmod 3$, has automorphism group which is complete of order $3.p^6$. Further, the smallest odd order any complete group may have is $3 \cdot 7^6 = 352,947$ and occurs when $p = 7$ and $P = GAP(7^5, 38)$.

Heiko Dietrich
(University of Auckland, h.dietrich@math.auckland.ac.nz)

Minimal conjugation families for finite groups

In 1967, Alperin introduced the concept of a conjugation family for a Sylow subgroup S of a finite group G. He proved that the normalisers of the non-trivial subgroups of S control its fusion, that is, elements in S which are conjugated in G are conjugated under elements in these normalisers. A famous example of a conjugation family is the Alperin-Goldschmidt conjugation family. In our work we consider conjugation families of minimal cardinality. In particular, we determine the unique minimal conjugation families for the symmetric groups and the finite groups of Lie type. In 1979, Alperin and Broue defined conjugation families for blocks of finite groups. We are able to generalise our results to this more general context.

This is joint work with Jianbei An (University of Auckland).

Sunanda Dixit
(University of Auckland, s.dixit@math.auckland.ac.nz)

A study on differentiable submanifolds

Topologically, a differentiable manifold is a manifold having a globally defined differential structure on it. Submanifolds are certain subsets of a manifold with the subspace topology. But what makes a differentiable submanifold of a differentiable manifold? In my presentation I will explain the above point and discuss the solution of a problem relating to it.

This is joint work with Prof. David B. Gauld (University of Auckland).

Peter Donelan
(Victoria University, peter.donelan@msor.vuw.ac.nz)

Geometric Jacobians and the singularity locus of a regional manipulator

The kinematics of a serial robot manipulator with k components can be expressed as a product of exponentials $\prod_{i=1}^{k} \exp(q_i X_i)$ in the 3–dimensional Euclidean group $SE(3)$. Here X_i is a *twist*, or 6-vector in the Lie algebra, representing the ith joint and q_i the joint variable defining its motion. The infinitesimal capability of the manipulator in the home configuration ($q_i = 0$ for all $i = 1, \ldots, k$) is determined by the geometric Jacobian matrix whose columns are the twist vectors. However as the robot moves the relevant twist vectors change. There is a way to write these new twists, themselves exponentials of the adjoint or bracket operators of the X_i, as a finite sum, using their minimal polynomials. As a result we obtain a complete closed form expression for the geometric Jacobian. As an application, an expression for the singularity locus of a regional manipulator ($k = 3$) is obtained that is quite general, in that the joints may have any form and the coordinates of the wrist centre are themselves parameters. We illustrate some of the bifurcations that can occur in the singularity locus.

Graham Donovan
(University of Auckland, g.donovan@gmail.com)

Modelling the asthmatic lung

Loss of lung function in asthma is thought to involve many complex phenomena and interconnected underlying causes. In particular, in asthmatic airway hyper-responsiveness, wherein the airways constrict too severely in response to stimulus, hypothesised underlying causes span multiple spatial scales. As such it is insufficient to take a reductionist approach, wherein each subsystem (at a given spatial scale) is considered in isolation and then the whole is taken to be merely the sum of the parts; there can be significant and important interactions and synergies between spatial scales. We present details of a multiscale, mathematical model the lung, specifically of asthmatic airway hyper-responsiveness, linking events ranging from the molecular scale to the level of the entire lung.

Rodney Downey
(Victoria University, rod.downey@vuw.ac.nz)

Generic case decision problems

Classical complexity using things like P, NP etc. seems often the wrong model for actual behaviour of problems. For example, consider the Simplex Algorithm, Polynomial Identity Testing and the like. Other models such as parameterized complexity (Downey-Fellows), average case complexity (Gurevich-Levin), smoothed analysis (Spielman-modern version of average case) may or may not apply, the latter two being very difficult to work with as you need to find the distributions. In 2003, a new method was suggested by Kapovich, Miasnikov, Schupp and Shpilrain mainly in the context of group theory. They called it *generic case complexity*.

The idea is that we have some kind of algorithm that works on a set of (Borel) density 1, and is *never wrong*, but could be partial. For example, any finitely presented group, and likely finitely generated group you fall over, will have a linear time generically decidable word problem.

This methodology presents unique problems to the computability theorist. I will survey the recent work of Jockusch and Schupp on this and give some new results from work jointly with those authors. This includes a new characterization of low c.e. sets using density and computability.

Nicholas Duncan

(University of Cambridge, UK, duncan.nicholas@gmail.com)

Toposes in geometry

A topos is often considered to be a category of set-like objects. However, a topos can also be considered as a generalized geometric space. Many geometric objects have an associated topos, for example every topological space has an associated topos of sheaves.

For some theories of geometry a topos can be constructed which represents that type of geometry. These toposes are called gros toposes. The gros Zariski topos from algebraic geometry is an example. Each object inside a gros topos represents a geometric object. Associated to each of these individual objects is another topos, called the petit topos. The differing viewpoints between the petit and the gros toposes correspond to two different approaches to algebraic geometry, the scheme approach and the functor of points approach.

In this talk I will cover the relation between the gros topos of geometric objects and the petit toposes of single geometric objects, with the example of categories arising from semialgebraic geometry.

Tatiana Evans

(Massey University, t.evans@massey.ac.nz)

Conditions for discreteness of groups of Möbius transformations

I will begin with a brief overview of hyperbolic 3-manifolds and discrete groups of Möbius transformations. I will then focus on recent results (joint work with Gaven Martin) which give conditions on a set of parameters associated to a 2-generator group of Möbius transformations that ensure that the group is discrete.

Shannon Ezzat

(University of Canterbury, shannon.ezzat@pg.canterbury.ac.nz)

Representation growth and exceptional primes

Representation growth is the study of counting the number of $n \times n$ complex irreducible representations of a group G. The case when G is a finitely generated nilpotent group has been studied, notably by Christopher Voll. He discovered that the p-local representation growth zeta function satisfied a very nice functional equation for almost all primes p. The methods used by Voll do not allow us to study these exceptional primes. In this talk we look at a method of studying these exceptional prime zeta functions along with some results.

Luke Fullard

(Massey University, l.fullard@massey.ac.nz)

Modelling the initiation of a hydrothermal eruption

Hydrothermal eruptions are a stunning phenomenon of nature. They occur in geothermal fields where a two-phase mixture of liquid water and water vapour lie at or very near boiling point conditions. Some pressure drop at the ground surface causes an initiation of boiling, leading to ejection of boiling water and rock/soil. In this talk I will discuss the development of a shock-tube based model aimed at predicting the initiation of such an eruption, present some preliminary results that predict the minimum pressure drop needed for an eruption to develop, and examine the way forward in hydrothermal eruption modelling.

Steven Galbraith

(University of Auckland, s.galbraith@math.auckland.ac.nz)

Hot topics in mathematics of public key cryptography

Public key cryptography was invented in the 1970s. Since that time there has been an enormous amount of research. I will summarise some of the original proposals from the 1970s and indicate the main strands of research since that time. The majority of the talk will survey recent work in cryptography based on two branches of number theory: elliptic curves over finite fields and lattices.

David Gauld

(University of Auckland, d.gauld@auckland.ac.nz)

Jordan and Schoenflies in non-metrical analysis situs

This is joint work with Alexandre Gabard of Genève and has been supported by the Marsden Fund Council from Government funding, administered by the Royal Society of New Zealand.

In 1887 Camille Jordan published his *Cours d'analyse de l'École Polytechnique* vol. III: *Calcul Intégrale* and included his famous *Jordan Curve Theorem*: every simple closed curve in the plane divides the plane into two parts each having the curve as its frontier. A couple of decades later Arthur Schoenflies proved moreover that for such a curve there was a homeomorphism of the plane sending the unit circle onto the curve.

I shall describe our proofs of versions of these theorems applicable to arbitrary surfaces. In particular, given any simply connected surface F and simple closed curve in F there is an embedding of the unit disc in F taking the bounding circle to the disc.

I shall also give applications of these theorems to dynamics, including a version of the hairy ball theorem for a wide class (of cardinality $2^{\aleph_1}$!) of surfaces of which the familiar two sphere $\mathbb{S}^2$ is the only compact (connected) example.

Rod Gover

(University of Auckland, gover@math.auckland.ac.nz)

Some geometry of PDE and compactifications of Einstein geometries

Given a differential geometric structure, such as a pseudo-Riemannian manifold, a conformal or projective structure, there is naturally associated to it many differential equations. Given a solution of such an equation, an interesting question is: what is the new geometric structure which arises from the combination of the original geometry plus the solution? For a large uniformly described class of equations there is a systematic approach to this that yields a rich theory with links to algebraic geometry. Among the applications is a canonical approach to geometrically treating the compactification of geometries.

Yousaf Habib

(University of Auckland, yhabib@math.auckland.ac.nz)

Corruption and remedies

General linear methods for ordinary differential equations are multistage and multivalue methods. Multistage means that, like Runge–Kutta methods, more than one evaluation of the differential equation function is performed in each time-step. Multivalue means that, like multistep methods, more than one piece of information is passed between steps. We are interested in general linear methods for long time integration of differential equation systems possessing quadratic invariants. This gives rise to the concept of *G*-symplectic methods.

General linear methods, like all multivalue methods, are prone to parasitic behaviour. This causes the multivalue solution to generate large errors and this leads to a loss of qualitative features of the underlying system. The corruption of the numerical solution can, however, be managed by controlling the parasitic growth parameter. Some remedies will be discussed and supporting numerical results will be presented.

John Hannah

(University of Canterbury, john.hannah@canterbury.ac.nz)

Reflecting on teaching linear algebra

Linear algebra is a vital advanced course for students of mathematics, science or engineering. But is the traditional approach to teaching this course as effective as we would like? In this talk we will describe how we went about introducing experiments and language skills into a second year linear algebra course. The research reported here is based on Schoenfeld’s framework of Resources, Orientations and Goals (ROGs). This focuses on the professional development viewpoint: how personal reflection and discussion leads to an increased awareness of one’s own ROG; how this influences lecturing-in-the-moment and decision-making; and the tensions between the lecturer as a mathematician and as a teacher. (Joint work with Sepideh Stewart and Mike Thomas, Auckland).

Emily Harvey

(University of Auckland, emily@math.auckland.ac.nz)

Designing experiments using mathematical models

Oscillations in the intracellular concentration of calcium are of interest as they are known to control a variety of cellular processes, from muscle contraction to neuronal firing. It has been suggested that the physiological mechanisms underlying these oscillations can be determined by means of a simple experiment in which a pulse of inositol trisphosphate (IP_3) is applied to the cell; however, more detailed mathematical investigations have shown that the situation is more complex than first thought. I will outline why this is and will present some recent work towards developing a novel experimental protocol, using mathematical models of the calcium dynamics.

Shaun Hendy

(Victoria University, shaun.hendy@vuw.ac.nz)

Effective rate constants for nanostructured heterogeneous catalysts

There is currently a high level of interest in the use of nanostructured materials for catalysis. With precious metal catalysts such as platinum in high demand, the use of these materials in nanoparticle form can substantially reduce the cost of the catalyst through the exposure of more surface area for the same volume of material. However, under diffusion-limited conditions i.e. conditions where the reaction may be at least partially inhibited by the speed in which the reactant must diffuse to active sites on the catalyst, high surface area and a high density of active sites may bring diminishing returns as sites consume reactant faster than it arrives. Here we apply a mathematical homogenisation approach to derive simple expressions for the effective reactivity of a nanostructured catalyst under diffusion limited conditions. When highly active catalytic sites, such as step edges or other defects are present, we show that distinct limiting cases emerge depending on the degree of overlap of the reactant depletion zone about each site. In gases, the size of this depletion zone is approximately the mean free path of the gas molecules, so the effective reactivity will depend on the structure of the catalyst on that scale.

Jeffrey Hunter

(Auckland University of Technology, jeffrey.hunter@aut.ac.nz)

Mixing and hitting in Markov chains

The expectation of the time to reach a state sampled from the stationary distribution of a discrete time finite Markov chain, when the chain starts in an arbitrary state, is shown to not depend on the initial starting state. This constant, recently named Kemeny's constant, has been shown to be a useful measure of "the time to mixing" in the Markov chain. It has been shown that the variance of the mixing time does, however, depend on the starting state. The distributional and moment properties of this mixing time random variable, and the related "random hitting time" random variable (when mixing can occur at the initial state) are explored in detail. The application of these results to perturbed Markov chains, when the transition probabilities are subjected to small changes, is also discussed.

Alex James

(University of Canterbury, alex.james@canterbury.ac.nz)

Can beetles prove that God exists?

Type Bombardier beetle into google and you'll suddenly find yourself in the middle of the Creationism/Evolution debate - Is there any science behind the hype? We try and explain how a mathematical model can help us understand how a tiny creature can defend itself from a Bluejay by firing acid at 100°C from its rear end and why they might have something in common with the WWII doodle bugs.

Stephen Joe

(University of Waikato, stephenj@math.waikato.ac.nz)

Sobol′ sequences with 'good' two-dimensional projections

A numerical technique for approximating integrals over the s-dimensional unit cube is to make use of quadrature points from Sobol′ sequences. An implementation of such a technique may be found in Algorithm 659 in the Collected Algorithms of the ACM. The original implementation was extended by Joe and Kuo in 2003 to go from 40 dimensions to 1111 dimensions. This involved using more primitive polynomials and finding more so-called 'direction numbers'.

This extended implementation did not guarantee that all the two-dimensional projections were 'good'. Since there are certain applications in which the integrands are of low effective dimension, it would be useful to have Sobol′ sequences with better two-dimensional projections.

This talk gives an outline of our ideas for finding new direction numbers up to dimension 21201 which attempt to achieve this. This is based on treating Sobol′ sequences as a special case of (t,s)-sequences in base b.

This is joint work with Frances Kuo of the University of New South Wales.

Ernie Kalnins

(University of Waikato, math0236@waikato.ac.nz)

Quantum superintegrability on Euclidean space

A technique is presented on how to show that the quantum analogues of classically superintegrable systems have more than enough differential symmetry operators. Superintegrable classical systems in n dimensions have $2n-1$ constants of the motion that are globally defined and polynomial in the momenta. This work has been done in conjunction with Willard Miller (Minnesota) and Jonathan Kress (Sydney).

Kamonwan Kocharoen

(Chiang Mai University, Thailand, kamonwan@chiangmai.ac.th)

Stability analysis of skeletal muscle model in Myotonia and periodic paralysis

Myotonia and periodic paralysis are caused by abnormalities in channels on skeletal membrane. Abnormalities are related to a tubular concentration of potassium and proportion of non-inactivating sodium channels. In this work, we modified a Hodgkin-Huxley model approach to inherit disorders of channels. We reformulated a sodium-current term in a T-tubule membrane compartment. Then we analyzed a stability of this modified model by investigating a formation of bifurcation. The tubular concentration of potassium and the proportion of non-inactivating sodium channels are designated as bifurcation parameters. In conclusion, this study illustrates a criterion on an existence of bifurcation to understand the ion channel diseases.

Mihaly Kovacs

(University of Otago, mkovacs@maths.otago.ac.nz)

Finite element approximation of the Cahn-Hilliard-Cook equation

We study the Cahn-Hilliard equation perturbed by additive coloured noise also known as the Cahn-Hilliard-Cook equation. We show almost sure existence and regularity of solutions. We introduce spatial approximation by a standard finite element method and prove error estimates of optimal order on sets of probability arbitrarily close to 1. We also prove strong convergence without known rate. This is joint work with Ali Mesforush and Stig Larsson, Chalmers University of Technology, Sweden.

Carlo Laing

(Massey University, c.r.laing@massey.ac.nz)

Bifurcations of lurching waves in a thalamic neuronal network

We consider a two-layer, one-dimensional lattice of neurons; one layer consists of excitatory thalamocortical neurons, while the other is comprised of inhibitory reticular thalamic neurons. Such networks are known to support “lurching” waves, for which propagation does not appear smooth, but rather progresses in a saltatory fashion; these waves can be characterized by different spatial widths (different numbers of neurons active at the same time). We show that these lurching waves are fixed points of appropriately defined Poincaré maps, and follow these fixed points as parameters are varied. In this way we are able to explain observed transitions in behavior, and, in particular, to show how branches with different spatial widths are linked with each other.

Satinee Lertprapai

(Burapha University, Thailand, satineel@buu.ac.th)

Comparison of the population variance estimators of exponential distribution by multiple criteria decision making method

In this paper we study the problems of estimation for the population variance of 1- and 2-parameter exponential distributions. There are six estimators of 1-parameter exponential distributions, and five estimators of 2-parameter exponential distributions. The purpose of this study is to compare the estimators based on the Multiple Criteria Decision Making (MCDM) procedure in order to obtain the best estimator.

Gerrard Liddell

(University of Otago, gliddell@maths.otago.ac.nz)

The structure of Lie quadratics

This talk will introduce non-linear approximations to general Lie quadratics, and show how these lead to a description of the "center" manifold.

Afshin Mardani

(University of Auckland, a.mardani@math.auckland.ac.nz)

A sufficient condition for topological spaces to be ω_1-squat

I will introduce the concept of $D-squat$ for a topological space X when D is a directed set, and I will present a sufficient condition on topological spaces X to be ω_1-squat, where ω_1 is the set of all countable ordinals.

Ben Martin

(University of Canterbury, B.Martin@math.canterbury.ac.nz)

Spherical buildings and the Centre Conjecture

A powerful tool for studying a group G is to construct a geometric object on which the group acts. Jacques Tits introduced the notion of a spherical building, which is constructed by glueing Euclidean spheres together. Spherical buildings have played an important part in understanding a large class of groups, including the reductive algebraic groups and the finite groups of Lie type. The Centre Conjecture of Tits asserts that certain subsets of a spherical building admit a point which is fixed under building automorphisms. In this talk I will discuss a recent approach to the Centre Conjecture using ideas from geometric invariant theory. This is joint work with Michael Bate (York) and Gerhard Röhrle (Bochum).

Robert McKibbin

(Massey University, R.McKibbin@massey.ac.nz)

Mathematical modeling of aerosol transport: effect of dispersion coefficients on predicted ground deposits

Aerosols ejected into the atmosphere by volcanic or hydrothermal eruptions, dust- or sand-storms, and particles from industrial emissions or other pollution sources, are dispersed by turbulent atmospheric wind currents. Generally, particle sizes are not uniform and may change during flight. The wind's speed, direction and dominant turbulence length scales may also change with elevation and with time. Some particles may be trapped on crop or forest foliage as they near the ground. Here, all of these changes are regarded as negligible; instead the focus is on the role of the dispersion coefficients in the solutions of the governing equations.

A quantitative model that regards both wind and particle settling speed as uniformly constant is outlined. The vertical, transverse and longitudinal dispersion coefficients are then each assumed to be separately zero, and the effects on the calculated ground deposits are compared and discussed. It is shown that neglect of vertical dispersion produces profiles that lack the characteristic long downwind tail of observed deposits. Neglect of transverse dispersion produces narrow deposits. Without longitudinal dispersion, the particle motion is not physically realistic, even though the predicted deposit distribution coincidentally has features that are similar to that predicted when all dispersion coefficients are non-zero.

Maarten McKubre-Jordens

(University of Canterbury, maarten.jordens@canterbury.ac.nz)

Real analysis in paraconsistent logic

This talk presents recent work on analysis of the real line using an inconsistency-tolerant (paraconsistent) logic. A basic introduction to paraconsistent logics will be given. We show that basic field and compactness properties hold, by way of novel proofs that make no use of consistency-reliant inferences. While inconsistency at the level of algebraic operations on the real number field cannot be contained (at least in the current formulation), it does not necessarily trivialize the system of real numbers, leaving open other prospects for non-nonsensical contradiction.

Ross McPhedran

(University of Sydney, ross@physics.usyd.edu.au)

Bandgaps in Structured Media: Part 2 – the Navier and biharmonic equations, phononic and platonic bandgaps

The development of the mathematics and physics of waves in photonic bandgap systems has been paralleled by investigations into equivalent structures for elastodynamic waves satisfying the Navier equation, leading to the concept of phononic bandgap materials. Quite recently, this has been adapted to the related case of elastic waves in structured thin plates, associated with platonic bandgap systems. This is the case of bending waves, and reduces to the solution of the biharmonic equation.

I will review the key differences between the elastodynamic and electromagnetic cases. I will use the biharmonic equation to exhibit a system whose dispersion equation and band diagram can be reduced to a simple form, leading to analytic predictions for the frequency limit of the fundamental bandgap, and for the nature of all higher bandgaps.

Michael Meylan

(University of Auckland, meylan@math.auckland.ac.nz)

The long and short of elastic wave interaction with platonic clusters

We show how to calculate scattering of flexural waves by platonic clusters in the time domain. We consider two cases, in the first the system is excited by a plane wave which is incident from infinitely far away. In the second case, we consider arbitrary initial conditions. For this case, we show that the solution in the time domain can be written as the sum of incident waves from all directions and we use circular rather than plane waves for ease of computation. We show that we can use an analytic extension of our problem to calculate the resonances (complex scattering frequencies) of the system. These allow us to calculate approximate solutions which are accurate for large times. We also discuss the early time behaviour of flexural waves, and show that the arrival time of the wave pulse is unaffected by the scatterers.

This is joint work with Prof. Ross McPhedran.

Klas Modin

(Massey University, K.E.F.Modin@massey.ac.nz)

Generalised Euler equations and image template matching

The field of geodesics on Lie groups started in the seminal work by Vladimir Arnold, who in 1966 produced a novel interpretation of the Euler equations in fluid dynamics as the geodesic equation on the group of volume preserving diffeomorphisms with respect to an invariant metric. Arnold realised that the same approach could be used to derive equations on any Lie group of finite or infinite dimension. Since then the research on generalised Euler equations has grown explosively. Many well-known equations of mathematical physics are now realised to be generalised Euler equations.

In this talk we show how the framework of generalised Euler equations can be applied to diffeomorphic shape and image matching, where one shape or image is warped into another by a smooth transformation. We give some recent results on the generalised Euler equation for conformal transformations. Inspired by the famous British biologist D'Arcy Thompson, we then show how shape/image transformation techniques can be used to study relationship between fish species.

Fabien Montiel

(University of Otago, fmontiel@maths.otago.ac.nz)

Experimental validation for numerical models of ocean wave interactions with sea-ice

A series of wave tank experiments, involving floating thin-elastic plates, have recently been conducted at École Centrale de Nantes in collaboration with the University of Otago. The experiments are aimed at validating the extensive linear theory, which has been used to model the propagation of ocean waves through clusters of sea-ice floes and appears in the scientific literature. A canonical model of wave scattering by a single ice floe will be presented. This involves potential theory and an eigenfunction matching method. Its experimental counterpart will be discussed in terms of the choice of the substitute material for sea-ice and the measuring devices. To finish, a comparison will be made between a selection of the theoretical and experiments data.

Rua Murray

(University of Canterbury, rua.murray@canterbury.ac.nz)

Polynomial decay of correlations

For a mixing dynamical system (T,X,m), a natural and important issue is the speed at which ensembles of initial conditions relax to equilibrium. This is quantified by asking how quickly the correlation integrals

$$C_n(f,g) := \left| \int f(x)\, g\circ T^n(x)\, dm(x) - \int f(x)\, dm(x) \int g(x)\, dm(x) \right|$$

decay to 0, for f and g belonging to certain regularity classes. Slow mixing occurs when T supports coherent structures which are "almost invariant" for long times. On the other hand, many "toy systems" have fast mixing (correlations decay exponentially); for example, uniformly hyperbolic systems, certain geodesic flows, many billiard systems, logistic maps, Henon maps and so on. Identifying precise rates of mixing is usually example specific, and difficult.

In this talk I'll describe a natural geometric generalisation of the usual Baker's map on the square. Each transformation is determined by the graph of a measurable "cut function" on $[0,1]$. For each $a > 0$ we can choose a simple cut function such that $C_n(f,g) = O(1/n^a)$ for Holder continuous f and g. All the maps are non-uniformly hyperbolic, but Bernoulli, with a familiar formula for the (measure theoretic) entropy. As well as describing aspects of the proofs, comparisons will be made with other standard approaches to the analysis of non-uniformly hyperbolic systems.

This talk reports joint work with Chris Bose, UVic (Canada).

Laurence Palk

(University of Auckland, l.palk@math.auckland.ac.nz)

Fluid flow and calcium dynamics in secretory epithelia

The parotid gland is the largest of the salivary glands. Parotid acinar cells are responsible for regulating saliva secretion. Calcium dependent ions channels maintain an ionic gradient which enables water to flow by osmosis into the saliva ducts. Dysregulation of fluid secretion can lead to conditions such as xerostomia, whereby sufferers do not produce enough saliva to comfortably eat or speak. We construct a mathematical model of the parotid acinar cell with the aim of investigating the effect of calcium dynamics and ion channel distribution on the fluid flow through the cell.

Judy Paterson

(University of Auckland, j.paterson@auckland.ac.nz)

Examining the use of questions in lectures: Ideas from the Datum project

A group of four mathematicians and four mathematics educators are collaborating in the fine-grained examination of selected short sections of video recordings of lectures drawing on Schoenfeld's KOG framework of teaching-in-context. We seek to examine ways in which this model can be extended to examine university lecturing and to promote and facilitate professional development. In this talk we will examine the discussion that grew out of one mathematician's interest in examining her use of questions and handling of student input during lectures. A second mathematician subsequently used an innovative technique of creating a revision lecture based on student questions submitted by email. While it is difficult to attribute causality, the sequence of peer observation, discussion and reflection surrounding these events seems to produce a strong argument for the effectiveness of the process as a means of supporting discipline-related lecturer professional development.

Mike Paulin

(University of Otago, mike.paulin@stonebow.otago.ac.nz)

Mechanical design for agility in the Otago Fishing Spider, Dolomedes aquaticus

The pursuit predator Dolomedes is an example of an evolved – i.e. locally optimal – solution to the problem of agile legged locomotion. We will present data, analysis and dynamical simulations detailing the mechanical design and kinematics of this animal. Dolomedes is a rigid body linkage with relatively simple joint kinematics; most joints have only 1df. A hydraulic mechanism controls the extension and elastic stiffness of leg joints, which is a power-law function of joint angle. Negative work done by backward-directed ground reaction forces is elastically stored in the joints and used to do positive work later in the gait cycle. Tapered, curved hairs under the feet can be modelled as massless springs which ensure that there are no impulsive forces (and therefore no energy is lost) in making or breaking ground contacts. In theory such a structure can move over uneven terrain in such a way that ground reaction forces do only positive work. We conclude that a well-designed leg can be as efficient and as simple to control as a wheel, but is more versatile (it's hard to grab a fly with a wheel).

Edoardo Persichetti

(University of Auckland, e.persichetti@math.auckland.ac.nz)

Compact McEliece keys based on Quasi-Dyadic Srivastava codes

The McEliece cryptosystem, based on algebraic coding theory, is a natural candidate for post-quantum cryptography. It has a very fast and efficient encryption procedure, and no known vulnerabilities against quantum computers. The original McEliece, introduced in 1978, is built upon binary Goppa codes. Though resistant against all known attacks, it has one big flaw, the size of the public key, that is much larger than the others, such as RSA, based on number theory problems. This makes the scheme impractical for many applications; thus, the latest research has focused on finding a way to significantly reduce this size. Recent proposals suggest to use codes with particular structures: two examples are dyadic matrices and quasi-cyclic codes. Very good results have been achieved, with keys as small as 512 bytes; unfortunately, modifying the structure of the codes exposes the cryptosystems to structural attacks, that aim to exploit the hidden structure in order to recover the private key. Almost all of the variants presented so far have been broken. Our scheme is based on Generalized Srivastava codes and represents a generalization of the Quasi-Dyadic scheme proposed by Misoczki and Barreto, with two advantages: a better flexibility, and improved resistance to all the known attacks.

Hung Pham

(Victoria University, hung.le.pham@msor.vuw.ac.nz)

Homomorphisms from Fourier algebras

Fourier algebras are generalizations of (the images of) the Fourier transform on the real line or the circle to general locally compact groups. They are commutative Banach algebras and are preduals of the group von Neumann algebras. In this talk, we will give a description of the contractive homomorphisms from each Fourier algebra into another Fourier(-Stieltjes) algebra.

Busayamas Pimpunchat

(No affiliation, pimbusaya@hotmail.com)

Complete oxygen depletion from rivers due to pollution

There is a growing concern about water quality worldwide. Among several tools, mathematical modelling has been extensively used to predict water quality and to provide reliable tools for water quality management in affected areas. In this work, we present a mathematical water quality model to analytically and numerically study the alleviation of pollution by aeration within a river. The model is composed of a pair of coupled reaction-diffusion-advection equations for the pollutant and dissolved oxygen concentrations, respectively. A steady-state model is mainly analytically considered and making connection to real situations was present. Such a model and its solutions may act as an aid to decision-making about restrictions to be imposed on farming and urban practices as well as water quality management. Analytical solutions of the simplified model and simulations enable scenarios to be tested for complete oxygen depletion and fish survival in rivers due to pollution, which is usually taken as above 30% of the saturated dissolved oxygen concentration.

Agate Ponder-Sutton

(University of Canterbury, agate.ponder-sutton@pg.canterbury.ac.nz)

Preliminary results of modelling Tradescantia fluminensis

Tradescantia fluminensis Vell. (Commelinaceae) is a concerning invasive weed within Australasia. The aim of this work is to use branching process models (a stochastic method for simulating multiple cases of individual, independent growth) to examine the interactions and population dynamics of T. fluminensis and different types of biological control agents. The model will be utilized to explore possible management strategies, and ask the question: “What are the overall probabilities of survival given a range of branching rates and death rates?” In this talk, the branching process model will be described and preliminary results presented. Some conclusions about the model in relation to field data will be discussed.

Dan Popovici

(Université Paul Sabatier, France, popovici@math.ups-tlse.fr)

Limits of projective and Moishezon manifolds under holomorphic deformations

We show that if all the fibres, except one, of a holomorphic family of compact complex manifolds are assumed to be either projective or Moishezon (i.e. bimeromorphic to projective ones), then the central fibre must be Moishezon. These statements had been conjectured since Hironaka showed by an example in 1962 that the central fibre need not be Kähler even if all the other fibres are projective, when the fibre dimension is at least 3. The work of Moishezon then provided a natural candidate for the way projectiveness degenerates in the deformation limit, but a proof had remained lacking since then. Our method is to construct Kähler metrics on the projective generic fibres in a well-chosen integral De Rham cohomology class, respectively to study the properness of the irreducible components of the relative Barlet space of divisors contained in the fibres when the generic fibre is Moishezon. We introduce new metrics, that we term “strongly Gauduchon metrics” as they generalise the classical Gauduchon metrics on the fibres and use them to show mass boundedness for the Kähler metrics (when the generic fibre is projective), respectively volume boundedness for the relative divisors in a given irreducible component (when the generic fibre is Moishezon).

Claire Postlethwaite

(University of Auckland, c.postlethwaite@math.auckland.ac.nz)

Bifurcations of heteroclinic cycles

Heteroclinic cycles are solutions of differential equations consisting of a set of saddle-type equilibria and connecting orbits. Generically they are of high codimension but they are known to occur robustly in systems with symmetry. Conditions for stability of even simple heteroclinic cycles are surprisingly complicated, and no general theorem has yet been established. In this talk I will review some of the mechanisms by which heteroclinic cycles can change stability and present some new results.

Christopher Poulton

(University of Technology, Sydney, chris.poulton@uts.edu.au)

Bandgaps in Structured Media: Part 1 – the Helmholtz equation and photonic bandgaps

There has been much recent research in the physics and mathematics communities into the properties of waves in strongly scattering, periodic media. This has been sparked by the demonstration that, if the scattering is sufficiently strong, there exist regions of frequency in which no wave propagation is possible, regardless of the wave direction. These regions are known as bandgaps, and have been used in a wide range of applications in the field of photonics, for the confinement of light and the modification of radiation properties of sources.

I will review the underlying mathematics of the bandgap phenomenon, and will discuss research aspects such as: unusual propagation characteristics within allowed bands, Green's functions and density of state functions, the basis of Bloch functions and defect states within the bandgaps.

Kiri Pullar

(University of Otago, kiripullar@gmail.com)

Signal transduction of electric fields in sharks: examination of ampulla microstructure using Finite Element Method (FEM)

The ampullae of Lorenzini are thin, gel-filled canals distributed over sharks' heads. According to conventional theory the canals form a low-resistance pathway such that the voltage across the sensory epithelium is approximately equal to the potential difference through the head parallel to the canal. Since a canal may be 10 cm long and the epithelium is about 10 microns thick, the canal amplifies the field strength by a factor of about 10,000. Recently, an alternative theory hypothesizes the gel has high impedance and the receptor cells measure potential gradients that develop within it. The protein channel molecules that transduce imposed fields to cell membrane potentials are thought to be located at the tips of cilia that project from epithelial cells into the gel. The geometry of these projections and the electrical characteristics of the materials must have a substantial effect on electric field strengths near the receptor molecules. Although there is considerable uncertainty about the electrical parameters, finite element modelling allows us to compare possible field strengths under the two different hypotheses across a plausible region of parameter space, and determine whether either of them can explain the remarkable sensitivity of sharks to weak electric fields.

This is joint work with Mike Paulin.

Iain Raeburn

(University of Otago, iraeburn@maths.otago.ac.nz)

Hilbert modules, orthonormal bases and Cuntz families

A Hilbert module over a C^*-algebra A is an analogue of a Hilbert space in which the coefficients come from A and the inner-product takes values in A; a Hilbert bimodule is a right Hilbert module which carries also a left action of A. We will discuss a family of Hilbert bimodules associated to self coverings of compact spaces in which the underlying right module is free, and how this freeness gives rise to families of isometries which satisfy a relation known as the Cuntz relation.

Tertius Ralph

(University of Auckland, tral001@aucklanduni.ac.nz)

The transient motion of a floating body

We consider the time-domain problem of a floating half-immersed horizontal circular cylinder of radius a. This is the simplest and best studied problem in the interaction of water waves and floating bodies. The motion of the body is constrained to heave only, subject to the linear equations of water waves and body motion. Viscosity and surface tension are neglected. While this problem has been well studied, there are still unanswered questions about the long time behaviour of the system and this is the principal focus of our investigation.

Because of the simple geometry of the body, we are able to use multipole expansions to solve for the displacements of the body in the frequency domain. We then use a generalized eigenfunction solution, which has been recently developed, in which the time-domain problem can be solved using the frequency domain solutions. We present numerical results for the heaving cylinder, and compare our results with previous results.

Benjawan Rodjanadid

(Suranaree University of Technology, Thailand, benjawan@sut.ac.th)

An iterative method for finding common solutions of generalized mixed equilibrium problems and fixed point problems

In this paper, we introduce an iterative method for finding a common element of the set of solutions of a generalized mixed equilibrium problem and the set of common fixed points of a finite family of nonexpansive mappings in a real Hilbert space. Then, we prove that the sequence converges strongly to a common element of the above two sets. Furthermore, we apply our result to prove three new strong convergence theorems in

fixed point problems, mixed equilibrium problems, generalized equilibrium problems and equilibrium problems.

Manfred Sauter

(University of Auckland, m.sauter@math.auckland.ac.nz)

The Volterra operator as a $*$-algebra generator

The classical Volterra operator V on $L^2(0,1)$ is defined by

$$(Vf)(t) = \int_0^t f(s)\,ds.$$

We study the extremal behaviour of the Volterra operator as a $*$-algebra generator. One remarkable result is that the $*$-algebra generated by V^2 and V^{*2} is dense in the whole scale of Schatten-class spaces, which includes the spaces of trace-class, Hilbert–Schmidt and compact operators.

Finally we discuss open questions and natural directions for further investigation.

This is joint work in progress with Tom ter Elst and Jaroslav Zemánek.

Charles Semple

(University of Canterbury, charles.semple@canterbury.ac.nz)

Submodular functions and optimizing biodiversity

One of the fascinations of mathematics is that common notions frequently arise in an unexpected settings. Recognizing such occurrences and then exploiting the theory of the common notion, often leads to elegant arguments and results. In this talk, we describe such a fascination in the context of optimizing biodiversity, where the common notion arising is submodular functions. This is joint work with Magnus Bordewich (Durham University).

Louise Sheryn, Megan Clark

(University of Auckland, l.sheryn@math.auckland.ac.nz)

Collective dreaming: A school-university interface

In 2008 the New Zealand Institute of Mathematics and Its Applications (NZIMA) funded a project to take a hard look at mathematics education in the four years from the last two years of secondary education to the first two years of undergraduate university education. The structure, pedagogy and content of mathematics in this period have been largely driven by tradition and particular interest groups. However not only has mathematics changed, but also the student body has changed, the teaching and lecturing body has changed, the reasons people study the mathematical sciences have changed, and the mathematical preliminaries have changed. The prime aim of the project was to get mathematical science senior secondary teachers and undergraduate lecturers to talk to each other. Such communication has not happened before in New Zealand on a large scale, and the ongoing discourse is couched in terms of blame and complaint. We explain why the project overcame these obstacles, and describe the emerging vision.

Alla Shymanska
(Auckland University of Technology, alla.shymanska@aut.ac.nz)

Modelling in charged particles optics using generating functions and Monte Carlo methods

A computational method for simulation of stochastic processes of an electron multiplication in microchannel electron amplifiers is developed. The method is based on MC simulations and theorems about serial and parallel amplification stages proposed here. The expressions for the mean gain and variance of the amplitude distribution at the output of the amplifier are obtained.

Splitting a stochastic process into a number of different stages, enables a contribution of each stage to the entire process to be investigated. The method preserves all advantages of MC simulations which are used only once for one simple stage.

The use of the theorems allows to conduct any further investigations and optimizations without additional MC simulations. The method provides a high calculation accuracy with minimal cost of computations.

The method is used to show how the input ratio signal/noise is transforming to the output one. The expressions for calculating the noise factor of a single channel and an array of the channels are obtained. Finally, the dependence of the average gain and the noise factor on the energy of the input electron beam is calculated.

Ivo Siekmann
(Auckland Bioengineering Institute, ivo.siekmann@auckland.ac.nz)

MCMC estimation of Markov models for ion channels

Ion channels are proteins which regulate the flow of ions across the cell membrane and within living cells. When triggered by the membrane potential or a ligand which binds to the channel, the ion channel opens for specific ions. More precisely, signals like voltage or ligands increase or decrease the open probability of the channel which behaves inherently stochastic. The statistics of ion channels can be represented by continuous-time Markov models (CTMM), however, translating a time series of open and closed currents measured from a single ion channel to a CTMM remains a challenge. Bayesian statistics combined with Markov chain Monte Carlo (MCMC) sampling provide means for estimating the rate constants of a CTMM directly from single channel data. In this talk, a new approach for the MCMC sampling of Markov models is presented. The new method detects overparametrisations and gives more accurate results than existing MCMC methods. It shows similar performance as QuB-MIL which indicates that it also compares well with maximum likelihood estimators. Data collected from an inositol trisphosphate receptor is used to demonstrate how the best model for a given data set can be found in practice.

Michael Smith

(University of Auckland, msmi162@aucklanduni.ac.nz)

Scattering by cavities of arbitrary shape in an infinite plate and associated vibration problems

In this talk a solution is presented for the displacement of a uniform elastic thin plate with an arbitrary cavity. The problem is formulated in terms of a system of boundary integral equations, with the unknowns expanded in terms of a Fourier series at the boundary. At the edge of the cavity free edge, simply supported and clamped boundary conditions are considered. Methods to suppress ill-conditioning are discussed and the Combined Boundary Integral Equation Method is outlined to control this problem. A connection is made between the problem of an infinite plate with an arbitrary cavity and the vibration problem of an arbitrary shaped plate by exploiting the jump phenomena present in single-layer distributions.

Sepideh Stewart

(University of Auckland, stewart@math.auckland.ac.nz)

A tactile innovative method of teaching introductory Markov Chain Monte Carlo (MCMC)

Teaching MCMC simulation is often carried out by presenting an algorithm, applying it to an example and translating it into an appropriate computer program. This approach however, overlooks some of the conceptual development that would help students grasp the subject. In this talk we show how starting from a discrete parameter space in the context of a Bayesian paradigm, MCMC can be understood conceptually. This is achieved when a two state discrete parameter is used within a tactile simulation where a coin supplies the proposal values and a die the acceptance-rejection probabilities. For those students who take the Bayesian approach towards mathematical inverse problems a disconnection between how discrete and continuous parameters are treated can be solved by this unifying method.

This is joint work with Wayne Stewart.

Teeranush Suebcharoen

(Massey University, teeranush_019@yahoo.com)

A model for cell-growth with asymmetric cell division

Many cell-division processes do not produce equal-size daughter cells. For example *C. elegans* and *Drosophila* embryos. During cell division, one daughter cell receives most or all of the localized molecules (usually proteins or mRNAs), while the other daughter cell receives less (or none) of these molecules. This results in two different daughter cells, which then take on different cell fates based on differences in gene expression. A partial differential equation which describes the growth, asymmetrical division and death for a cell population structured by size is examined. We consider a cell division model where a cell divides into a number of different-sized daughter cells. We have used DNA content as a measurement of size in this model. In this talk, we assume that each cell divides into β_1 and β_2 daughter cells and $\beta_1 > \beta_2 > 1$ with constant rate and the parameters for growth and mortality are constant. The non-local differential equation for the steady-size probability distribution of the population is derived from the partial differential equation which has an exact solution in the form of a Dirichlet series. Also it is shown that this solution is the unique probability density function that solves the non-local differential equation . Conditions are established which determine the long-term behaviour of the population.

Winston Sweatman

(Massey University, w.sweatman@massey.ac.nz)

Deformations while jet stripping steel coatings

In the process of sheet steel production, a metallic alloy coating is added to the steel surface for corrosion protection. At the mathematics-in-industry study group (MISG2009) and in subsequent work, we considered an approach in which the steel is pulled through a bath of molten alloy. Coating thickness is controlled using air knives after leaving the bath. Recently, coating developments have led to surface quality problems. Models and results will be presented.

Rachael Tappenden

(University of Canterbury, rachael.tappenden@pg.canterbury.ac.nz)

Extensions of compressed sensing

We consider the restoration of signals and images which are a combination of a piecewise constant function plus a sparse component. A new algorithm is presented which aims to reconstruct signals of this type from a limited set of observed data. The algorithm is broken down into two subproblems which both involve minimization of an $l1$-regularized least squares problem. Numerical results are presented which demonstrate the effectiveness and efficiency of the proposed method.

Chyou Te-yuan

(University of Otago, teyuan.chyou@gmail.com)

Passive dynamic walking and control on level ground

I have been working on an uncontrolled humanoid-like biped that is capable of walking passively on downhill using gravity, and also on the level ground by avoiding inelastic foot collisions. By consideration of the energy, a passive gait on level ground cannot be stable. In this presentation we discuss control forces that can be applied to re-stabilize the unstable collision-free gait after being perturbed by a change in ground height and we evaluate the energy cost of these forces.

Tom ter Elst

(University of Auckland, terelst@math.auckland.ac.nz)

Partial Gaussian bounds for degenerate differential operators

Let S be the semigroup on $L_2(\mathbf{R}^d)$ generated by a degenerate elliptic operator, formally equal to $-\sum \partial_k c_{kl} \partial_l$, where the coefficients c_{kl} are real bounded measurable and the matrix $C(x) = (c_{kl}(x))$ is symmetric and positive semi-definite for all $x \in \mathbf{R}^d$. Let $\Omega \subset \mathbf{R}^d$ be a bounded Lipschitz domain and $\mu > 0$. Suppose that $C(x) \geq \mu I$ for all $x \in \Omega$. We show that the operator $P_\Omega S_t P_\Omega$ has a kernel satisfying Gaussian bounds and Gaussian Hölder bounds, where P_Ω is the projection of $L_2(\mathbf{R}^d)$ onto $L_2(\Omega)$.

Similar results are for the operators $u \mapsto \chi S_t(\chi u)$, where $\chi \in C_b^\infty(\mathbf{R}^d)$ and $C(x) \geq \mu I$ for all $x \in \operatorname{supp} \chi$.

This is joint work with El Maati Ouhabaz.

Robert Thompson

(University of Otago, rthompson@maths.otago.ac.nz)

Unmasked: The science of cloaking

Metamaterials are artificial materials engineered to possess certain properties, including some that may not be found in nature such as a negative index of refraction. The development of metamaterials has led to several novel applications, including optical cloaking. The recent construction and demonstration of an actual cloaking device has conjured dreams of Harry Potter's cloak of invisibility and has garnered lots of media attention.

Transformation optics is a method of designing optical devices based on visualizing the desired behavior of electromagnetic fields; and basically constitutes an inverse problem: Given a desired electromagnetic field behavior, what material parameters are required to realize that behavior? Together, transformation optics and metamaterials are a powerful combination, as virtually any desired field behavior can now be realized by employing metamaterials.

Using the particular example of cloaking, I will describe metamaterials and discuss a newly developed approach to transformation optics. This new approach clarifies the action of transformation optics while simultaneously making transformation optics more useful by broadening its domain of applicability.

Puntip Toghaw

(Kasetsart University, Thailand, tiptoghaw@yahoo.com)

A model of GLP1-DPP4 interaction accounts for glycemic improvement after bariatric surgery.

Many publications reported a marked improvement of glycemic control in obese patients with type 2 diabetes who underwent bariatric surgery for weight loss, especially gastric bypass and biliopancreatic diversion (BPD). After surgery, the blood glucose profile is improved before any significant weight loss. There are several plausible hypotheses to explain the rapid, weight-independent glycemic improvement. In addition, some papers provide evidence supporting the ghrelin hypothesis and the lower intestinal hypothesis, but some of them support the upper intestinal hypothesis. Thus, the results of the above hypothesis testing have not been clear. Therefore, in order to examine these hypotheses, we developed a mathematical model of the oral glucose tolerance test (OGTT) that incorporates the GLP1-GIP-DPP4and the hormone ghrelin interaction to glucose-stimulated insulin secretion. The model is used to describe the blood glucose profile before and after gastric bypass in complementary ways for improving glucose control.

Christopher Tuffley

(Massey University, c.tuffley@massey.ac.nz)

Intrinsic linking of n-complexes

In 1983 Conway and Gordon proved that, no matter how the complete graph K_6 is embedded in $\mathbb{R}^3$, the embedding is guaranteed to contain a pair of cycles that form a nontrivial link. This fact is expressed by saying that K_6 is *intrinsically linked*. Since then Flapan and other authors have shown that embeddings of larger complete graphs are forced to exhibit more complicated linking behaviour, such as n-component links, or 2-component links with high linking number. I will show that many of these results can be extended to embeddings of complete n-complexes in $\mathbb{R}^{2n+1}$, using Taniyama's extension of Conway and Gordon's result to embeddings of the complete n-complex on $2n+4$ vertices in $\mathbb{R}^{2n+1}$.

Bruce van Brunt

(Massey University, b.vanbrunt@massey.ac.nz)

A singular Sturm-Liouville Problem arising from a cell growth model

The basic cell growth model developed by Hall and Wake in 1989 is based on a Fokker-Planck type partial differential equation with zero dispersion. A separation of variables process leads to a pantograph equation of the type

$$y'(x) + ay(x) = a\alpha y(\alpha x),$$

where a and $\alpha > 1$ are constants. In this model, y is required to be a probability density function and $y(0) = 0$.

A more general version of the pantograph equation is

$$y'(x) + ax^n y(x) = \lambda \alpha^n x^n y(\alpha x),$$

where $n \geq 0$ is an integer and λ is an eigenvalue parameter. The above equation leads to a singular Sturm-Liouville problem. In this talk we study the problem and show that the eigenvalues are simple and that the eigenfunctions can be determined in terms of Dirichlet series. The eigenfunctions can be used in the original partial differential equation problem to obtain explicit solutions for a broader class of boundary conditions.

Graeme Wake
(Massey University, g.c.wake@massey.ac.nz)

Calculus from the past and at a distance

There are many problems which give rise to situations where cause and effect are separated in time, space, age and/or size. To our detriment, these equations are rarely studied in the curriculum yet they possess a rich framework by which many different phenomena can be analysed. Maybe they should be in the curriculum? Little systematic theory has been developed to help solve these problems. This talk will be a personal account of representative generic problems I have encountered in different applications over four-and-a-half decades of such problems in both bounded and unbounded domains. They come from areas as diverse as chemical engineering, population biology and genetics. Some problems will be solved and others will be left as “coffee-room teasers”. This talk is aimed at non-expert problem-seekers.

Neil Watson
(University of Canterbury, n.watson@math.canterbury.ac.nz)

A unifying definition of a subtemperature

The potential theory of the heat operator

$$\Theta = \sum_{i=1}^{n} \frac{\partial^2}{\partial x_i^2} - \frac{\partial}{\partial t}$$

in $\mathbb{R}^{n+1}$, is now well developed, but it has been developed in two different ways. First there was the harmonic space approach of Bauer, and second the heat ball approach of myself. Later, Bauer proved the equivalence of the two approaches. More precisely, he showed that the subsolutions in the two theories – the subcaloric functions and the subtemperatures – are the same. He used relatively sophisticated results from both theories. In this talk, I shall outline a new approach using a new definition of subtemperature. This unifies the theory from the outset, as the two earlier definitions arise as characterizations of subtemperatures, almost simultaneously.

Phil Weir
(University of Otago, pweir@maths.otago.ac.nz)

Applications of an FEM approach for the analysis of sea-ice hydroelasticity

An examination is presented of the response to regular and irregular incident sea waves by ice floes. Finite element methods are applied to the 2D time-dependent hydroelastic problem, both in the beam and in the potential flow. The coupled problem is formulated in a cleanly articulated manner, where beam and fluid models are independently interchangeable and the vertical motion of the beam supplies boundary conditions for the fluid potential. This description enables the use of interchangeable beam models and allows larger deformations to be considered than linear theory would permit.

We take a mesh-based, time-stepping approach, applying a predictor-corrector method to find the combined motion of the body and fluid at each timestep. This leads to an extensible formulation able to accommodate a wider variety of physical properties than is possible using the frequency domain techniques predominant in sea-ice research. Thus we provide for more robust, physically realistic models of polar ice floes. Further, the versatility of our method provides a numerical testing ground to obtain useful qualitative results at low mesh resolutions. At each time-stepping iteration, we solve both for the beam and fluid using standard finite element techniques, through the open source FEM package, FEniCS.

Graham Weir
(Industrial Research, g.weir@irl.cri.nz)

Comparison between impacts of macro-sized and nano-sized idealised elasto-plastic particles with a large hard surface

In this talk we analyse plastic collisions between spherical macro-sized and nano-sized particles and a large hard plane. We assume that for the nano-sized particles, surface tension between the particle and plane accelerates the particle to a speed which is large compared with its initial speed. The subsequent maximum width and depth of plastic indentation of the nano-sized particle by the plane is independent of the initial speed of the particle, being a function of particle size, and material properties. This depth of indentation is independent of particle size. If this depth is assumed equal to one interatomic spacing in the colliding particle, then a relationship is derived linking nano-size yield strength to the elastic modulus of the particle. Similarly, should surface tension overcome the elastic recoil process so that the particle is captured on the surface of the plane, then the period of the surface oscillations of the particle depends on the particle size and on material properties.

Ben Whale
(University of Otago, ben.whale@otago.ac.nz)

Functional definitions of pseudo-Riemannian distance suitable for noncommutative geometry

A currently growing area of research in noncommutative geometry is the search for generalisations to pseudo-Riemannian manifolds. A key ingredient in any generalisation is a functional formulation of Lorentzian distance. Current results along these lines are only proven for a very special subclass of Lorentzian manifolds and all proofs exploit an eikonal condition. This talk will demonstrate the full applicability of eikonal based arguments and show what additional structure is needed when such arguments fail.

Michael Whittaker

(University of Wollongong, mfwhittaker@gmail.com)

Poincaré duality for hyperbolic dynamical systems

Noncommutative Poincaré duality for a pair of C^*-algebras was formulated by Kasparov to generalize the notion of Poincaré duality for topological spaces. Hyperbolic dynamical systems, known as Smale spaces, will be introduced along with two C^*-algebras associated with a Smale space. I will show that these C^*-algebras are Poincaré dual and discuss some consequences. This is joint work with Jerry Kaminker and Ian Putnam.

Timothy Williams

(-, timothy.williams@bristol.ac.uk)

Shear waves in elastic solids with microscopic imperfections or inclusions

In this talk I will discuss the propagation of long elastic shear waves in media consisting of microstructures such as fibres, cavities and cracks in an otherwise isotropic medium. Examples of applications of this topic could be in wave propagation in fibre-reinforced media and cortical bone.

The medium is modelled as being a tesselation of repeated rectangular cells containing a certain number of these microstructures, and the microstructures are all aligned parallel to the direction of polarization of the wave. We solve this problem in the long wave limit by using the method of asymptotic homogenization.

The equations that must be solved in a doubly-periodic two-dimensional space are Laplace's equation and a boundary condition involving the normal derivative of the unknown function. A particularly interesting mixed boundary condition is generated when considering a fibre that has become partially debonded from its host medium.

The governing equations are very similar to those that need to be solved in water wave problems when finding the radiation potential due to the forced oscillation of a rigid body in a fluid.

Wenjun Zhang

(University of Auckland, wzha122@math.auckland.ac.nz)

Criticality of Hopf bifurcation in excitable systems

Excitable systems are used to model many biophysical processes, including changes of action potentials in neurons and changes of intracellular calcium concentration in various cell types.

In this talk we are mainly concerned with Hopf bifurcation in such excitable systems. Hopf bifurcation occurs at the transition between equilibrium and periodic solution. The criticality of the Hopf bifurcation indicates the stability of the periodic solution, and therefore plays an important role in the overall dynamics.

Surprisingly, naive application of standard techniques can give misleading information of the criticality of the Hopf bifurcation in an excitable system. We examine general excitable systems to show how a naive approach may fail and how to obtain a correct result by a refined method. The idea is then applied to some classic biophysical models including Belousov-Zhabotinsky and Hodgkin-Huxley models.

Posters

Maryam Alavi-Shooshtari, David Williams, Jennifer Salmond and Jari Kaipio

(University of Auckland, m.alavi@math.auckland.ac.nz)

Decision theoretic approach to the analysis of self-referencing sensor networks

Due to the increasing availability of sensors of moderate cost, sensor networks are currently considered for different tasks. One of these is the monitoring of air quality with several, possibly hundreds of sensors that cover an extensive area. Due to practical problems related to calibration and failure detection by external reference measurements, a self-referencing approach is mandatory to make extensive sensor networks practically realizable. Such approaches have not been published earlier. We consider a decision theoretic approach for the detection of local disturbances, which may be due either to actual changes in the environment or to malfunction of the sensors. The approach is based on modelling the measurement process as a multivariate time series and constructing a bank of approximate Wiener filters that predict each individual measurement process. Based on the statistics of the related prediction error processes, a decision rule is established, that fixes the false alarm rate. As an application, we consider the performance of the approach with two year air quality data sets from Houston, Texas and Vancouver, Canada. We show that relatively small changes of individual sensor measurements can be detected with high probability.

Alona Ben-Tal

(Massey University, a.ben-tal@massey.ac.nz)

Simplified model of rhythm generation in the intact respiratory neural network

Rhythm generation in the respiratory neural network is complex. Under normal conditions it involves several interacting populations of neurons but under severe conditions (for example lack of oxygen) rhythm is effectively generated by a single population. The transition between the normal and severe cases is accompanied by changes in the neural signals appearance and frequency. To help understand the underlying dynamics, a minimal phenomenological model has been developed and will be presented.

Sunanda Dixit, David Gauld

(University of Auckland, s.dixit@math.auckland.ac.nz)

Study on smooth non-metrisable manifolds

A differentiable manifold is a topological manifold with a globally defined differential structure on it. It has been established that some manifolds admit more than one non-diffeomorphic (i.e., different) differential structures. The non-metrisable manifolds, the long line $\mathbb{L}$ and the open long ray $\mathbb{L}_+$ play vital roles in providing important counter examples in topology. It has been verified that $\mathbb{L}_+$ supports $2^{\aleph_1}$ non-diffeomorphic

differential structures on it. The poster will present some of the initial explorations regarding differential structures (i.e.,smoothings) on the product manifold $\mathbb{L}^2_+$ in the quest for other non-product smoothings.

Atheer Matroud

(Massey University, a.a.matroud@massey.ac.nz)

NTRFinder: An algorithm to find nested tandem repeats

We introduce the algorithm NTRFinder to find complex repetitive structures in DNA that we call nested tandem repeats (NTRs). We have tested our algorithm on both real and simulated data, and to date have found 3 NTRs of interest in real sequences.

Motivation: The ITS region of rRNA from Colocasia esculenta (taro), a plant of ethnobotanical interest, has been found to contain a 1600 bp complex repetitive structure consisting of two distinct tandem repeat motifs interspersed with one another. We propose that such "nested tandem repeats" are significant population markers and have developed the algorithm NTRFinder to search for NTRs in other sequences. A major issue is parsing, the determination of the optimal boundaries of the motifs, which is a significant problem in the analysis of NTRs.

Materials and methods: NTRFinder adapts Wexler et al's heuristic for finding tandem repeats to the problem of finding NTRs, and aligns and analyses them using an extension of Fischetti et al's wrap-around dynamic programming. The algorithm has been implemented in Java. We propose a model of motif duplication, mutation and deletion to explain the observed patterns. Under this model the parsing problem is solved using the most parsimonious tree linking the observed variants approximating each motif, minimising the number of duplicate substitutions in the development of the NTR.

Pingyu Nan

(University of Auckland, pnan011@math.auckland.ac.nz)

Reducing the dimension of mathematical models of physiological systems

Detailed models of physiological systems can contain a large number of variables, making analysis of the models difficult. Various ad hoc methods are commonly used to reduce the dimension of these types of models, with the aim being to capture the essential dynamics of the full model in a reduced system which is easier to analyze.

In the poster, some common reduction methods were shown in the context of reducing the dimension of the Hodgkin-Huxley equations. A recent progress on finding a helpful reduced version of a neural model may include.

Kate Patterson, James Sneyd, Edumnd Crampin, James Melvin, Ted Begenisich

(University of Auckland, National Institute of Health, University of Rochester, k.patterson@math.auckland.ac.nz)

Electrolyte exchange in the salivary duct

A healthy salivary gland secretes saliva in two stages. First, acinar cells generate primary saliva, a plasma-like, isotonic fluid high in Na^+ and Cl^-. In the second stage, as the fluid travels past duct cells, Na^+ and Cl^- are exchanged for K^+ and HCO_3^-, producing a hypotonic final saliva with no apparent loss in volume. This electrolyte exchange allows saliva to act as a buffer in the mouth, neutralizing acids and preventing potentially pathogenic microbial colonization. We construct a radially symmetric, three compartment model of the duct to examine this electrolyte exchange and fluid conservation.

Edoardo Persichetti

(University of Auckland, e.persichetti@math.auckland.ac.nz)

Public-key cryptography from coding theory

Cryptography is the science which studies the hiding of information. Its origins are very old: they date back to Julius Caesar himself. Computers made possible deeper levels of complexity, and allowed the encryption of any data which could be translated into binary. Thus, electronic communication like smart cards or the internet gave the whole field of study much more importance. Modern cryptography can be considered a distinct branch of mathematics. A relatively recent, and innovative, approach is Public-Key Cryptography. It is based on an "asymmetric" key scheme, consisting of a pair of keys: a public key for anybody to encrypt, and a private key used to decrypt. A threat for actual cryptography is the possibility of quantum computers: as soon as a machine of proper size is available, nearly all the current protocols won't be secure. In this sense McEliece's work, based on Coding Theory, was pioneering. His scheme has no known vulnerabilities against quantum computers, and has a fast and efficient encryption procedure. A drawback is the size of the public key, still too large for many applications. Our research focuses on the study of finite fields and coding theory, aiming at a compact representation of the code, to reduce the public key size without compromising the security.

Winston Sweatman, Steven Barry and Mark McGuinness

(Massey University, Australian National University, Victoria University, w.sweatman@massey.ac.nz)

Heat transfer during steel coil annealing

Cold rolled steel requires heat treatment (annealing) to release stresses and reform crystalline structure. The 2008 MISG in Wollongong modelled the process used by New Zealand Steel for which steel coils are heated in a batch annealing furnace. Determining the temperature within each coil is complicated by height-dependent gaps within the coils. Deciding on suitable boundary conditions for the outside of the coils provides a further challenge. A linear model was found sufficient to model the heating process.

Wenjun Zhang
(University of Auckland, wzha122@math.auckland.ac.nz)

Interaction of solitary pulses and periodic waves in calcium dynamics

Excitable systems of reaction-diffusion equations are used to model many biophysical processes, including changes of intracellular calcium concentration in various cell types. Understanding the interaction between solitary and periodic travelling waves is important in these systems.

Numerical computation often shows that there is a complex bifurcation structure related to the interaction of the solitary and periodic travelling waves in these excitable systems. We show how geometric singular perturbation theory can be used to determine the dynamics in a nearby singular limit and hence to explain some features of the complicated dynamics in the full system. We illustrate the method with models of intracellular calcium dynamics.